GENERAL SERVICES ADMINISTRATION
Washington, DC 20405

PBS P 3490.2

GSA POLICY AND PROCEDURE

SUBJECT: Document Security for Sensitive But Unclassified Building Information

1. Purpose. This directive describes GSA's policy to protect sensitive but unclassified (SBU) building information for GSA-controlled space. GSA-controlled space includes owned, leased, and delegated Federal facilities. Not all building information is automatically considered sensitive but unclassified. Only specific applicable information, marked with SBU designations, needs to be controlled in accordance with this policy. GSA will use SBU terminology and markings on all building information in all formats (see Appendix B). Both legacy SBU and new SBU building information will be subject to the terms of this directive.

2. Background. GSA has been marking and managing sensitive but unclassified building information and has issued several updates to the policy since the bombing of the Alfred Murrah Federal Building in 1995.

Executive Order 13556, signed on November 4, 2010, establishes a program for managing Controlled Unclassified Information, with the National Archives and Records Administration (NARA) serving as the executive agent. This Executive Order emphasizes "…the openness and uniformity of Government-wide practice." GSA has been working with NARA in developing Controlled Unclassified Information (CUI) standards and best practices. Upon completion of NARA's CUI efforts and directives (with expected implementation to start April 2016), GSA's SBU designation will be replaced with the NARA CUI designation and this directive will be updated to reflect the new CUI requirements.

3. Cancellation. PBS 3490.1A Document Security for Sensitive but Unclassified Building Information, issued June 1, 2009, is cancelled, effective immediately.

4. Scope and Applicability. This directive applies to the access to and generation, dissemination, storage, transfer and disposal of all SBU building information related to GSA-controlled space and to procurements to obtain, alter, or manage space, either Government-owned or leased, including GSA space that is delegated to other Federal agencies.

a. All sensitive building information shall be marked and managed as SBU in accordance with this directive.

i. General Services Administration Information Technology (GSA IT), along with PBS business lines, will develop a system to track project SBU building information, to be implemented in a phased approach and completed within five years of the issuance date of this directive.

b. Existing SBU documents shall be controlled under this directive when procuring and contracting for design and construction services for renovations to existing facilities. For new facilities, the building drawings and other related building information will be reviewed and may be designated SBU, as appropriate. This designation applies at the time SBU building information is turned over by the Architect-Engineering (A-E) personnel to the Government as part of the final construction control documents. However, not all building information will be designated as SBU.

THIS DIRECTIVE DOES **NOT** APPLY TO CLASSIFIED BUILDING INFORMATION, which is governed by Executive Order 13526 - Classified National Security Information.

5. Policy Objectives. This directive has three principal objectives:

a. To diminish the potential that building information will be available for use by a person or persons with an interest in causing harm, and

b. To allow access to this information to those recipients who have a legitimate business need to know such information.

c. To ensure a "Business Need to Know" exists. All individuals must have a legitimate purpose to handle SBU building information. They must use good judgment, common sense and take reasonable care to ensure that sensitive building information is protected in accordance with this directive.

6. Definitions.

a. "SBU building information" is information related to GSA-controlled space that is sufficiently sensitive to warrant some level of protection from full and open public disclosure, but does not warrant classification. This information requires safeguarding and dissemination controls in order to diminish the potential that building information will be accessible to a person or persons with an interest in causing harm. Appendix A provides a list of examples of SBU building information. This list is for illustrative purposes and is not comprehensive.

b. A "Business Need to Know" exists when access to SBU building information is necessary for the conduct of official GSA business. Some examples of individuals who may have a legitimate "business need to know" are GSA project managers, staff from the Office of the Inspector General (OIG), authorized vendors, utilities, state and local fire department personnel, among others. This directive does not describe all instances of a legitimate "business need to know".

7. Clarification of GSA Order CIO P 2181.1. All building drawings or building information should not be designated, automatically, as SBU. Refer to Appendix A of this document for guidance. GSA Order CIO P 2181.1 provides the policy and procedures for issuing and maintaining GSA credentials. Chapter 2, Section 4.b.(4) of GSA Order CIO P 2181.1 states, “Those individuals whose duties require a higher degree of trust, such as IT system administrators, those who handle financial transactions, or those who deal with PII, and other sensitive information (e.g., building drawings, etc.), will continue to require investigations associated with higher levels of trust such as the Minimum Background Investigation (MBI) or the Limited Background Investigation (LBI).” These requirements shall not be used to restrict access to SBU building information further than as clarified in Section 4 (Applicability) of this directive. Access to sensitive building drawings may be granted on a 'Business Need to Know' basis (as concurred on by the respective GSA business line) without regard to the credentialing cited above.

8. Signature.

/S/ September 2, 2014
NORMAN DONG
Commissioner
Public Buildings Service

PBS P 3490.2 Document Security for Sensitive But Unclassified Building Information

Table of Contents

GENERAL REQUIREMENTS AND RESPONSIBILITIES

The principles governing the management of SBU building information are as follows for all GSA personnel and contractors:

1. SBU building information shall be controlled so that building information in electronic and hard copy formats are made available only to individuals who have a legitimate business need to know (see Appendices A and B).

2. Adequate controls shall be used to monitor access to and dissemination of SBU building information.

3. SBU building information shall be safeguarded during use and either properly destroyed or returned to GSA after use.

4. SBU information shall not be presented in public forums.

5. The SBU designation of each building's information (for design, construction bidding, facility management, etc.) shall be based on the specific information's level of sensitivity and the physical security level of the building itself.

SPECIFIC REQUIREMENTS AND RESPONSIBILITIES

1. Public Buildings Service. The Public Buildings Service (PBS) is ultimately responsible for protecting SBU building information from unauthorized use and for making the initial determination of whether an entire building, or portion thereof, is considered sensitive.

2. PBS Regional Commissioners (RCs). PBS RCs or authorized designee (or in the case of delegated buildings, agency officials), make the initial determination regarding whether a building's documents/information or portion thereof are/is considered sensitive. That determination shall in turn trigger an action on the part of the PBS Project Manager or Program Manager to mark the necessary related building information as SBU.

   a. RCs shall consider the physical security level of the building itself, as well as comparable building types and occupants in making the determination whether or not a building's documents/information or portion thereof are/is sensitive.

   b. The RC shall designate an individual responsible for controlling SBU building information.

   c. RCs must implement this directive within their Regions in a uniform, consistent manner so that all items containing SBU building information are marked and handled appropriately.

   d. In the case of a new building in the planning stages, for a single tenant, the RC in consultation with the tenant will hold decision-making authority in determining the appropriate sensitivity of building information.

   e. In the case of a new building in the planning stages, for multiple tenants, the RC in consultation with all planned tenants will hold decision-making authority in determining the appropriate sensitivity of building information.

3. Tenants. In the case where the tenant or tenants require/s a greater sensitivity designation than for comparable building types and occupants, this tenant or group of tenants will be required to pay any extra costs associated with higher security requirements and less competition in procurement. The tenant/s will agree to fund such costs via rent, Reimbursable Work Authorization, etc., as applicable. Extra costs may be due to limits on Architect-Engineering (A-E) personnel access, bidding restrictions, reduced competition for construction or facility management, or other factors. The RC or designee will assist the tenant in identifying the cost of higher security requirements. Within a Federal campus, the SBU designation may apply to one or more buildings as needed, but will not automatically apply to all buildings within the same campus if any particular building(s) is (are) designated as SBU.

4. PBS Project Manager or Program Manager (PM). The PBS PM is responsible for reviewing all building documents, identifying and marking SBU building information, and

including instructions in Statements of Work (SOWs) for contractors to mark documents as SBU, if appropriate.

a. The PBS PM shall identify and mark as SBU, in electronic or paper formats, only the building information that meets the criteria for SBU, which must be controlled, as stated herein. The PBS PM shall refer to Appendix A of this directive for further guidance.

b. The PBS PM shall coordinate with various groups (tenants, stakeholders, the Facility Security Committee, etc.) on all matters pertaining to building information.

c. The PBS PM, in consultation with the Facility Security Committee (FSC), is responsible for reviewing all building information at every milestone where there is a change in the physical space or tenant, to validate SBU markings are correct and current.

d. If building information designation is found to be incorrectly marked or no longer required, the PBS PM shall follow the instructions related to Mandatory Review in paragraph 11 below.

5. Facility Security Committee (FSC). After construction is complete, FSC or its current equivalent, as established by the standards of the Interagency Security Committee (ISC), shall advise the PBS PM regarding specific building information where SBU markings are necessary.

a. When a building is not designated as sensitive, the FSC, or its current equivalent, may still determine that some specific building information must be controlled. In this case, the FSC shall advise the PM to mark only that specific building information as SBU. The FSC shall refer to Appendix A of this directive for further guidance.

6. Disseminators. Disseminators of SBU building information must comply with the all policy principles and requirements of this directive. SBU building drawings that are part of a procurement must be issued in accordance with FAR 5.102(a)(4) on the secure side of the FedBizOpps website (https://www.fbo.gov/), or any successor system, with proper document control protocols to allow legitimate registered vendors access to the documents for proposing and pricing the procurements.

7. Contracting Officers (COs). COs shall include the clause in Appendix C, or a similar updated clause per the General Services Administration Acquisition Manual (GSAM), in all solicitations (including Solicitations for Offers (SFOs)) and in all building contracts and/or final leases that may contain, require access to, or cause the generation of SBU building information. This applies to all contracts issued after issuance of this directive and implementation of the rule making process, whichever occurs later.

a. Examples of such contracts are A-E design, construction, facility management contracts, and related professional service contracts such as construction manager as agent (CMa) and Commissioning Agent (CxA) contracts.

b. COs must take appropriate action when they become aware that contractors have not fulfilled contractual obligations regarding the protection of SBU building information. Such action may include an investigation, referring the contractor for suspension or debarment proceedings, and/or terminating the contract for default.

8. GSA Employees. GSA Employees may disseminate SBU building information only after a proper review and the imprinting or affixing of a mark, as required by this directive (see Appendix B for marking guidance), and after determining that the recipient of SBU building information is authorized to receive such information before dissemination of that information.

9. General Counsel. The Office of General Counsel (OGC) provides legal advice concerning Freedom of Information Act (FOIA) requests that apply to SBU building information. OGC also provides counsel regarding the application of this directive.

10. All PBS Regional Commissioners, Assistant Commissioner and Deputy Assistant Commissioners must make their respective personnel aware of the requirements in this directive and require that their staffs be trained in the proper application of this directive, including encryption software applications available to GSA personnel and contractors.

11. Mandatory review. For building projects (for design, construction, facility management, etc.), the PBS PM is responsible for reviewing all building information which does or may contain SBU building information at regular milestones (such as change in use, configuration or tenant); the PBS PM is responsible for identifying and validating that SBU markings are correct and current. If building information designation is found to be incorrectly marked or no longer required, the PBS PM will correct the marking immediately or ensure that action is taken promptly to change or remove the marking.

12. Marking information. For any electronic or printed SBU building information created after the issuance date of this directive, pages containing SBU building information must have the markings shown in Appendix B imprinted or affixed.

13. Limiting dissemination to authorized recipients. SBU building information may be disseminated only after it is determined by GSA personnel that each recipient is authorized to receive it. The criterion to determine whether a recipient is authorized to receive SBU building information is that the recipient must have a legitimate business need to know, as further described in Section 4 (Scope and Applicability) of the transmittal for this directive.

a. Federal, State, and local government entities. GSA must provide SBU building information for the performance of official Federal, State, and local government functions, such as inspections, OIG audits, code compliance reviews and issuance of building permits, among other purposes. Public safety entities such as fire departments may require access to SBU building information on a ‘need to know’ basis. This directive must not prevent or encumber the dissemination of SBU building information to public safety entities.

b. Vendors, Nongovernment entities and utilities. Unless the action is exempt under FAR 4.1102, all disseminators are responsible for verifying that a contractor or contracting firm is currently registered as "active" in the System of Award Management (SAM) database at www.sam.gov and also has a legitimate business need to know SBU building information before releasing it to any contractor or firm. Nongovernment entities and/or utility companies may also require access to SBU building information for the performance of work on GSA-controlled space on a 'need to know' basis and do not necessarily need to register within the SAM database.

14. Electronic transmission of SBU building information. GSA employees, who electronically transmit SBU building information outside of the GSA network, must encrypt the data with an approved NIST algorithm, such as Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES), in accordance with Federal Information Processing Standards Publication (FIPS PUB) 140-2, Security Requirements for Cryptographic Modules. As email outside of the GSA network is not encrypted, GSA personnel working within the GSA network may only transmit SBU building information using GSA-approved encryption procedures. ("Within the GSA network" means inside the firewall, including Citrix and GSA VPNs.)

15. Dissemination of SBU building information in non-electronic form or on portable electronic data storage devices. Portable electronic data storage devices include but are not limited to CDs, DVDs, and USB drives. Non-electronic forms of SBU building information include paper documents.

a. By mail. GSA employees must utilize only methods of shipping that provide confirmation of receipt of the SBU building information, such as track and confirm, proof of delivery, signature confirmation, or return receipts.

b. In person. GSA employees must provide SBU building information only to authorized representatives of Federal, State, local government entities, SAM-registered firms, and others that have a legitimate business need to know such information.

16. Safeguarding SBU building information. GSA employees must not take SBU building information outside of GSA facilities, except as necessary for the performance of a GSA project. If a GSA employee takes SBU building information outside of a GSA facility, access to the information must be limited to those with a legitimate business need to know. Such information must be returned to a GSA facility or destroyed when no longer needed for the performance of a GSA project. GSA employees must not store or retain SBU building information on any electronic device or media not owned by GSA.

17. Destroying SBU building information. When SBU information, in any format, is no longer needed, SBU building information must be destroyed such that the information is rendered unreadable and incapable of being restored, in accordance with GSA CIO IT

Security 06-32, Media Sanitization Guide and Appendix A of NIST Special Publication 800-88, Guidelines for Media Sanitation. Alternately, the SBU building information may be returned to the CO.

18. Freedom of Information Act (FOIA) requests. SBU markings do not control the decision of whether to disclose or release the information to any entity that files a FOIA request. Any determination to disclose SBU building information, in accordance with a FOIA request, must be made after consultation with the servicing legal office.

19. Reporting incidents of concern. Any actual or suspected unauthorized disclosure of SBU information must be reported immediately to the CO for the related contract or the appropriate RC. RCs are required immediately to notify the FSC for the building involved. Any incident involving suspected computer or cyber security breach or attack, as defined by NIST Special Publication 800-61, Computer Security Incident Handling Guide, must be reported in accordance with the current version of GSA CIO P 2100.1, Information Technology (IT) Security Policy Order and GSA CIO IT Security Procedural Guide: CIO-IT Security-01-02, Incident Response (IR).

Appendix A. Examples of Sensitive But Unclassified Building Information

Not all building information is automatically considered Sensitive But Unclassified (SBU). After the PBS Project Manager (PM) has reviewed, identified, and marked SBU building information, then access to the information must be controlled. SBU building information may be contained in any document (including drawings, specifications, virtual modeling, reports, studies, analyses) and in any format with information pertaining to:

1. Location and details of secure functions or secure space in a building, location or space. Examples include:

   a. Prisoner or judges' secure circulation paths or routes (both vertical and horizontal).
   b. Detention or holding cells.
   c. Sally ports.
   d. Security areas, including but not limited to control rooms and incident command centers
   e. Building automation systems.
   f. Telephone and riser closets

2. Location and type of structural framing for the building, including any information regarding structural analysis. Examples include information related to:

   a. Progressive collapse.
   b. Seismic.
   c. Building security.
      i. Blast mitigation.
      ii. Counterterrorism methods taken to protect the occupants and the building.

3. Risk assessments and information regarding security systems or strategies of any kind. Examples include:

   a. Camera locations.
   b. Nonpublic security guard post information (e.g., number, location, operations, etc.).

Note: In the case of building information related to a specific suite, room/space, or other component that is designated as SBU (i.e. Building Automation System (BAS) diagram, security camera layout, etc.), the SBU designation does not necessarily carry over to the entire building, or to the entire campus.

Note: Building information for a stand-alone steam plant facility or similar service facility and its associated tunnels shall be designated SBU when it services a building that is designated SBU.

Appendix B. Sensitive But Unclassified Marking Information

1. Any electronic or printed document, pages containing SBU building information must have the following markings:

SENSITIVE BUT UNCLASSIFIED (SBU)
PROPERTY OF THE UNITED STATES GOVERNMENT
FOR OFFICIAL USE ONLY
Do not remove this notice
Properly destroy or return documents when no longer needed

2. The following mark must be affixed to the cover or first page of any document (such as the cover page on a set of construction drawings).

SENSITIVE BUT UNCLASSIFIED (SBU)
PROPERTY OF THE UNITED STATES GOVERNMENT
COPYING, DISSEMINATION, OR DISTRIBUTION OF THIS DOCUMENT TO UNAUTHORIZED RECIPIENTS IS PROHIBITED
Do not remove this notice
Properly destroy or return documents when no longer needed

3. The previous two markings must be prominently labeled in bold type in a size appropriate for the document or portable electronic data storage device or both, if applicable. On a set of construction drawings, for example, the statements must be in a minimum of 14 point bold type or equivalent.

4. The SBU markings must be used regardless of the medium through which the information appears or is conveyed.

Appendix C. SBU Contract Clause

Contracting Officers (COs) shall include the following clause, or a similar updated clause per the General Services Administration Acquisition Manual (GSAM), in: (1) all solicitations containing SBU building information (including Solicitations for Offers (SFOs)); and shall include the following clause in: (2) contracts and/or final leases that may contain, require access to, or cause the generation of SBU building information.

[Begin clause]

Safeguarding and Dissemination of Sensitive But Unclassified (SBU) Building Information

This clause applies to all recipients of SBU building information, including offerors, bidders, awardees, contractors, subcontractors, lessors, suppliers and manufacturers.

1. Marking SBU. Contractor-generated documents that contain building information must be reviewed by GSA to identify any SBU content, before the original or any copies are disseminated to any other parties. If SBU content is identified, the Contracting Officer (CO) may direct the contractor, as specified elsewhere in this contract, to imprint or affix SBU document markings to the original documents and all copies, before any dissemination.

2. Authorized recipients.

   a. Building information designated SBU must be protected with access strictly controlled and limited to those individuals having a legitimate business need to know such information. Those with a need to know may include Federal, State and local government entities, and nongovernment entities engaged in the conduct of business on behalf of or with GSA. Nongovernment entities may include architects, engineers, consultants, contractors, subcontractors, suppliers, utilities, and others submitting an offer or bid to GSA, or performing work under a GSA contract or subcontract. Recipient contractors must be registered as "active" in the System for Award Management (SAM) database at www.sam.gov and have a legitimate business need to know such information. If a subcontractor is not registered in the SAM and has a need to possess SBU building information, the subcontractor shall provide to the contractor its DUNS number or its tax ID number and a copy of its business license. The contractor shall keep this information related to the subcontractor for the duration of the contract and subcontract.

   b. All GSA personnel and Contractors must be provided SBU building information when needed for the performance of official Federal, State, and local government functions, such as for code compliance reviews and for the issuance of building permits. Public safety entities such as fire and utility departments may require access to SBU building information on a need to know basis. This clause must

not prevent or encumber the dissemination of SBU building information to public safety entities.

3. Dissemination of SBU building information:

a. By electronic transmission. Electronic transmission of SBU information outside of the GSA network must use session encryption (or alternatively, file encryption). Encryption must be via an approved NIST algorithm with a valid certification, such as Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES), in accordance with Federal Information Processing Standards Publication (FIPS PUB) 140-2, Security Requirements for Cryptographic Modules per GSA policy.

b. By nonelectronic form or on portable electronic data storage devices. Portable electronic data storage devices include, but are not limited to CDs, DVDs, and USB drives. Nonelectronic forms of SBU building information include paper documents, among other formats.

i. By mail. Contractors must utilize only methods of shipping that provide services for monitoring receipt such as track and confirm, proof of delivery, signature confirmation, or return receipt.

ii. In person. Contractors must provide SBU building information only to authorized recipients with a need to know such information. Further information on authorized recipients is found in Section 2 of this clause.

4. Record keeping. Contractors must maintain a list of all entities to which SBU is disseminated, in accordance with sections 2 and 3 of this clause. This list must include at a minimum: (1) the name of the State, Federal, or local government entity, utility, or firm to which SBU has been disseminated; (2) the name of the individual at the entity or firm who is responsible for protecting the SBU building information, with access strictly controlled and limited to those individuals having a legitimate business need to know such information; (3) contact information for the named individual; and (4) a description of the SBU building information provided. Once “as built” drawings are submitted, the contractor must collect all lists maintained in accordance with this clause, including those maintained by any subcontractors and/or suppliers, and submit them to the CO. For Federal buildings, final payment may be withheld until the lists are received.

5. Safeguarding SBU documents. SBU building information (both electronic and paper formats) must be protected, with access strictly controlled and limited to those individuals having a legitimate business need to know such information. GSA contractors and subcontractors must not take SBU building information outside of GSA or their own facilities or network, except as necessary for the performance of that

contract. Access to the information must be limited to those with a legitimate business need to know.

6. Destroying SBU building information. When no longer needed, SBU building information must be destroyed so that marked information is rendered unreadable and incapable of being restored, in accordance with guidelines provided for media sanitization within GSA CIO IT Security 06-32, Media Sanitization Guide and Appendix A of NIST Special Publication 800-88, Guidelines for Media Sanitization. Alternatively, SBU building information may be returned to the CO.

7. Notice of disposal. The contractor must notify the CO that all SBU building information has been returned or destroyed by the contractor and its subcontractors or suppliers in accordance with paragraphs 4 and 6 of this clause, with the exception of the contractor's record copy. This notice must be submitted to the CO at the completion of the contract to receive final payment. For leases, this notice must be submitted to the CO at the completion of the lease term. The contractor may return the SBU documents to the CO rather than destroying them.

8. Incidents. All improper disclosures of SBU building information must be immediately reported to the CO at _____<insert address and contact information>____ . If the contract provides for progress payments, the CO may withhold approval of progress payments until the contractor provides a corrective action plan explaining how the contractor will prevent future improper disclosures of SBU building information. Progress payments may also be withheld for failure to comply with any provision in this clause until the contractor provides a corrective action plan explaining how the contractor will rectify any noncompliance and comply with the clause in the future.

9. Subcontracts. The contractor and subcontractors must insert the substance of this clause in all subcontracts.

[End of clause]